AB&T Telecom LLC
CPNI Compliance Manual

Compliance Officer: Emmet Tydings
President
Direct Number: (240)654-1877

Table of Contents

INTRODUCTION

The Telecommunications Act of 1996 grants the Federal Communications Commission the authority to regulate the use and disclosure of customer proprietary network information ("CPNI"). Pursuant to this authority, the FCC has adopted a series of rules (the "CPNI Rules" or "Rules") requiring every provider of telecommunications services (including providers of VoIP services) to protect CPNI from unauthorized use or disclosure, and has used its power to enforce the CPNI Rules to give breadth and substance to those requirements.

Generally speaking, providers must take the following steps in order to comply with the CPNI Rules:

- Adopt policies and designate a senior executive to serve as Compliance Officer.
- Develop and implement a program designed to protect CPNI from unauthorized use and disclosure in accordance with the Rules.
- Develop and implement accountability standards and employee disciplinary procedures.
- Train employees regarding CPNI compliance and disciplinary action.
- Create and implement a monitoring and reporting mechanisms.
- Implement and maintain a process for reviewing and updating CPNI practices, procedures, and training materials.
- File an annual certificate of compliance and compliance support statement.

This Compliance Manual ("Manual") includes essential information and guidance regarding the use and disclosure of CPNI by AB&T Telecom employees. Every employee who is authorized to access or use CPNI is expected to follow the practices and procedures set forth in this Manual, and will be required to participate in annual CPNI training.

FCC enforcement of the obligations of providers to protect CPNI under the Rules is unwavering. Consequently, the FCC takes the position that *any* unauthorized use or disclosure of CPNI without proper authorization is considered a failure by the Company to comply with the Rules, and exposes the Company to the imposition of significant fines and penalties.

It is essential, therefore, that employees of AB&T Telecom LLC. ("AB&T Telecom" or the "Company") possess a basic understanding of the rules applicable to the use and handling of CPNI, and the practices and procedures described in this Manual. Any employee that fails to follow these practices and procedures will be subject to disciplinary action.

If you have any questions regarding application of these practices and procedures, or you encounter an issue that you believe is not adequately covered by the document, you should immediately contact the Compliance Officer for guidance, whose name and phone number are provided on the cover page of the Manual.

STATEMENT OF COMPANY POLICY

IT IS THE POLICY OF AB&T TELECOM LLC TO PROTECT CUSTOMER PROPRIETARY NETWORK INFORMATION FROM UNAUTHORIZED USE AND DISCLOSURE AS REQUIRED BY APPLICABLE LAW.

OVERVIEW OF THE CPNI RULES

- As noted above, providers of telecommunications services are prohibited from using, disclosing, or permitting access to CPNI unless authorized by the customer or the Rules. The Rules implement this requirement by: Defining the circumstances under which companies that provide telecommunications services (including providers of VoIP services) may use, disclose, or permit access to CPNI (47 CFR § 64.2005).
- Establishing the circumstances under which customer approval must be obtained before providers may use, disclose, or permit access to CPNI (47 CFR §64.2007).
- Setting the process by which customer approval must be obtained (47 CFR § 64.2008).
- Creating a set of minimum safeguards that providers must implement before using (§ 64.2009) or disclosing (§ 64.2010) CPNI.
- Requiring providers to notify customers in the event of a CPNI breach (47 CFR § 64.2011).

A|1. The Definition of CPNI.

A|1.1. CPNI is defined by **Section 222(h)(1) the Telecommunications Act of 1996** (the "Telecommunications Act" or "Act") as:

A|1.1.1. Information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and

A|1.1.2. Information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.

A|1.1.3. Examples of CPNI include information typically available from the details of a customer's monthly bill, such as the type of line, technical characteristics, class of service, current phone charges, billing records,
directory assistance and other service charges, usage data, and calling patterns.

A|1.2. The Telecommunications Act expressly excludes Subscriber List Information from the definition of CPNI. Customer List Information, which is subject to other rules and regulations, is defined by the Act as:

A|1.2.1. A customer's listed name, telephone numbers, addresses, and primary advertising classifications assigned when service is established, or any combination of such listed names, numbers, addresses, and classifications; and

A|1.2.2. Information that the provider has published, caused to be published, or accepted for publication in any directory format.

A|2. Customer Authorization Requirements Related to CPNI (47 CFR § 64.20 05).

A|2.1. The circumstances under which the Company and its Affiliates1 may use, disclose, or permit access to CPNI largely depends on the purpose, and on the nature of the Company's relationship to the customer.

A|2.2. Customer authorization is not required:

A|2.2.1. To provide services to an existing customer.

A|2.2.2. To market services to a customer, if such services are in the same category as other services currently subscribed to by such customer.

A|2.2.3. To permit an Affiliate to provide services to a customer, but only if the customer subscribes to more than one category of service offered by the Company.

A|2.2.4. To protect its rights and property, and to protect customers of affected services and other carriers from fraudulent, abusive, or unlawful practices involving such services.

A|2.2.5. To provide inside wiring installation, maintenance, and repair services.

A|2.2.6. As an interconnected VoIP provider, the Company is also permitted to market services previously known as "adjunct-to-basic" services to customers without their authorization, such as speed dialing and call forwarding.

A|2.3. Customer authorization is required:

A|2.3.1. To market products or services to a customer that are in a different category of services than those currently purchased from the Company by the customer.

A|2.3.2. To identify or track customers that call competing service providers.

A|2.3.3. If an Affiliate or agent of the Company wants to use CPNI to market new communications related products or services to a customer, and the customer is not a customer of the Affiliate.

A|2.3.4. To market non-communication related services, such as Customer Premise Equipment (CPE), or information services, such as Internet or Digital TV.

A|2.3.5. To market CPE and information services to a Customer that has not previously purchased CPE or communications services from the Company.

A|3. Pre-Authorization Notice Requirements (47 CFR § 64.2008).

A|3.1. Before requesting authorization to use, disclose, or permit access to a customer's CPNI, the Company must notify the customer that the customer has the right to restrict such use, disclosure, and access to the customer's CPNI.

A|3.1.1. Notification records must be kept for at least 1 year.

A|3.1.2. Notice must be provided on an individual basis.

A|3.1.3. Notice must be reasonably proximate to the Company's request for approval.

A|3.2. The FCC Rules impose both general and specific requirements for customer notices.

A|3.2.1. The notice must indicate the scope and duration of the Company's use of CPNI.

A|3.2.2. The notice must state that the customer has the right, and the Company has the duty under federal law, to protect the confidentiality of the customer's CPNI.

A|3.2.3. The notice must detail the steps to be taken by the customer to grant or withhold approval.

A|3.2.4. The notice must inform customers that a refusal to grant approval will not affect the customer's service (provided that the Company may briefly explain, in clear and neutral language, the direct consequences of withholding approval).

A|3.2.5. The notice must be clear, straightforward, not misleading, and otherwise sufficient to permit customer to make an informed choice.

A|3.2.6. The notice must state that with respect to services to which the customer is not currently subscribed, approvals and denials will remain valid until affirmatively revoked or limited by the customer.

A|3.2.7. If the notice is given in writing, it must be legible, and must be styled and placed so that it easily identified and seen by the customer.

A|3.2.8. If any portion of the notice is given in one or more different languages, then the entire notice must be given in those languages.

A|3.3. In addition to mandatory provisions, the Company has the option of including the following information in the customer notice:

A|3.3.1. Use of the customer's CPNI improves the ability of the Company to tailor products and services to the needs of the customer.

A|3.3.2. The customer may direct the Company to disclose customer CPNI to a third party by delivering such directive to the Company in writing. The notice may not, however, include a statement that encourages the customer to freeze third party access to CPNI.

A|4. Obtaining Customer Authorization (47 CFR § 64.2007).

A|4.1.1. Customer authorization may be obtained in writing or electronically. Authorization may also be obtained verbally, provided the Company can demonstrate that such verbal approval satisfies the requirements of the Rules.

A|4.1.2. The Company must document each instance in which customer authorization is obtained, and must keep a record of such authorization for at least one year from the date it is given.

A|4.1.3. Customer authorization remains effective until the customer revokes or modifies it.

A|4.1.4. If customer authorization is required but the manner for obtaining approval is not specified, then customer approval must be obtained using an "opt-in" approval2 method, which is discussed in more detail below.

A|5. "Opt-In" and "Opt-Out" Authorization (47 CFR § 64.2008).

A|5.1. A customer must affirmatively "Opt-in" before CPNI may be used or disclosed for the purpose of marketing services that are not "communications-related services."

A|5.1.1. Consent must be expressly confirmed with the customer's written or electronic signature.

A|5.1.2. Failure to respond to a request for authorization to use or disclose CPNI when "opt-in" consent is required is the same as a refusal to grant authorization.

A|5.2. The Company and its Affiliates may use CPNI to market communications-related services to a customer unless the customer chooses to "opt-out" of such use.

A|5.2.1. Notice must be communicated in writing or electronically, except in the case of "one-time" requests (below).

A|5.2.2. If the customer does not "opt-out" within thirty (30) days of the notice date, the customer is deemed to have consented to the use described in the notice.

A|5.2.3. If the notice is delivered electronically, the 30 day period begins on the date notice is sent. If notice is delivered in writing, the 30 day period begins on the third day following the mailing date.

A|5.2.4. The Company must repeat this type of notice every two years.

A|5.2.5. See Appendix 1 for a more thorough discussion of "opt-in" and "opt-out" compliance.

A|6. Email and "One-Time" Notices (47 CFR § 64.2008).

A|6.1. If notice will be given by electronic mail:

A|6.1.1. The Company must first obtain express, verifiable customer consent to receive service-related email.

A|6.1.2. The Company must permit reply directly by email in order to opt-out.

A|6.1.3. Email notices returned to the Company as undeliverable are ineffective for all purposes, and any follow up or additional notices must then be sent by another method in order to satisfy the Rules.

A|6.1.4. Subject lines must clearly and accurately state the purpose of the email.

A|6.1.5. Through one or a combination of methods, the Company must permit customers to opt-out on a 24/7 basis at no additional cost to the customer.

A|6.2. In cases where CPNI will only be used or disclosed one time:

A|6.2.1. Notice must satisfy the notice content requirements explained above, provided that the Company may omit certain disclosures if they are not relevant to the limited purpose for which the Company intends to use or share CPNI.

A|6.2.2. Oral notice is permitted, but only for the duration of the call in which such use is requested.

A|7. Use of CPNI: Mandatory Safeguards (47 CFR § 64.2009). In connection with the use of CPNI, the Company must: **a**

A|7.1. Implement a system that clearly establishes the customer's approval status before using, disclosing, or permitting access to CPNI in circumstances where customer approval is required.

A|7.2. Educate company personnel regarding the circumstances under which they are authorized to use CPNI.

A|7.3. Create and implement a documented disciplinary process applicable to cases of unauthorized use or disclosure of CPNI by Company personnel.

A|7.4. Maintain electronic or other legible records of Company and Affiliate sales and marketing programs that use CPNI for a period of 1 year. The records must include the details of:

A|7.4.1. CPNI disclosures to, or access to CPNI by, third parties.

A|7.4.2. A description of the marketing campaign and the specific CPNI used in the campaign.

A|7.4.3. The products and services promoted in the campaign.

A|7.5. Develop and implement an oversight program that includes:

A|7.5.1. Routine supervisory review of CPNI use.

A|7.5.2. Review of Company compliance with the Rules, including prior supervisory approval of all requests to use CPNI in outbound marketing campaigns.

A|7.5.3. Compliance records must be kept for a period of 1 year.

A|7.6. Annually file a compliance certificate3 specifically addressing procedures used by the Company to ensure compliance with the CPNI Rules, actions against data brokers, and customer complaints related to CPNI.

A|7.6.1. The certificate must be accompanied by a statement explaining how the Company's operating procedures ensure compliance with the Rules.4

A|7.6.2. The certificate must be signed by an officer of the Company with personal knowledge that such procedures have been implemented.

A|7.7. Notify the Commission by letter, in form and substance consistent with the provisions of the Rules, within 5 business days of any instance in which opt-out mechanisms fail, unless such failure is an anomaly. Notice is required even if the Company has offered customers alternative opt-out methods.

A|8. Disclosure of CPNI: Mandatory Safeguards (47 CFR § 64.2010). In connection with disclosing or permitting access to CPNI, the Company must:

A|8.1. Take reasonable steps to discover and protect against attempts to obtain unauthorized access to CPNI.

A|8.2. Properly authenticate customers prior to disclosing CPNI based on customer-initiated phone contact, online account access, or an in-store visit.

A|8.2.1. CPNI may only be disclosed over the phone in response to a customer initiated phone contact in which the customer provides a pre-determined password that is not prompted by a request for biographical or account information.

A|8.2.2. If the customer fails to provide the correct password, the Company may only provide call detail information to the customer by sending it to the customer's address of record, or by calling the customer's telephone number of record.

A|8.2.3. If the customer then initiates a call to the Company and accurately discloses call detail information without Company assistance, the Company is permitted to discuss the call detail information provided by the customer.

A|8.3. Online access to CPNI.

A|8.3.1. Prior to allowing online access to CPNI, customers must be authenticated by the Company without the use of readily available biographical information or account information.

A|8.3.2. Once authenticated, the customer may only obtain online access to CPNI by providing a pre-established password, again without prompting for readily available biographical information or account information.

A|8.4. Authentication and passwords.

A|8.4.1. To create a customer password, the Company must authenticate the customer without the use of readily available biographical information or account information.

A|8.4.2. Backup authentication methods may be used if the customer loses or forgets the password, provided the backup method does not prompt the customer for readily available biographical information, or account information.

A|8.4.3. If the customer cannot provide the correct password or the correct response for the back-up customer authentication method, the customer must establish a new password.

A|8.4.4. The Company may contractually agree with business customers to use other authentication regimes, provided the customer has both a dedicated account representative and a contract that specifically addresses the protection of CPNI.

A|8.5. Account change notifications.

A|8.5.1. the Company must immediately notify customers if the customer's password, required response for backup authentication, online account, or address of record is created or changed.

A|8.5.2. Notification may be provided by voicemail or text message to the phone number of

record, or by mail to the address of record, prior to such changes, and must not reveal any of the new information.

A|8.5.3. Notification is not required if the customer is initiating service or selecting an initial password.

A|9. Notification of CPNI Breach (47 CFR § 64.2011).

A|9.1. A "breach" occurs when a person intentionally accesses, uses, or discloses CPNI without required authorization.

A|9.2. Within 7 business days of reasonably determining that a breach has occurred, a Company must notify the FBI and the US Secret Service (the "Agency Notice"). The FCC maintains a link for this purpose at http://www.fcc.gov/eb/cpni.

A|9.3. The Company may not notify its customers or disclose the breach publicly, either voluntarily or pursuant to state or local law or the Rules, prior to or for a period of 7 full business days from the date the Company files the Agency Notice (the "Blackout Period"), *unless*:

A|9.3.1. The Company includes states in the Agency Notice that the Company believes that delay will result in immediate and irreparable harm to affected customers, consults with the relevant investigating agency, and cooperates with the efforts of such agency to mitigate any adverse consequences of providing notice to customers; or

A|9.3.2. For reasons related to national security or a criminal investigation, the relevant agency directs the Company in writing to refrain from notifying customers until agency approves such notice.

A|9.3.3. the Company must notify customers of a breach as soon as the Blackout Period expires or the Company is authorized to deliver such notice by the relevant investigating agency, as described above.

A|9.3.4. For a period of 2 years from the date a breach is discovered, the Company must maintain an electronic or other tangible record of such breach, and the applicable Agency Notice and customer notification. The record must include, if available, discovery and notification dates, a detailed description of affected CPNI, and the circumstances that lead to the breach.

AB&T TELECOM
CPNI COMPLIANCE
PRACTICES AND PROCEDURES

B|1. Management Controls.

B|1.1. All employees who are or may be required to use or access CPNI in the course of performing their jobs will receive annual CPNI training.

B|1.1.1. Annual CPNI training will include a review of the CPNI Rules, AB&T Telecom's CPNI policies and procedures, and any changes to the CPNI rules, AB&T Telecom's policies and procedures, or both that have been implemented during the preceding year. Employees will be required to demonstrate proficiency with the material by successfully completing a review examination in connection with annual training.

B|1.1.2. New employee and remedial training will be offered on an as-needed basis.

B|1.2. An officer of the Company will be identified to act as the Compliance Officer for CPNI purposes, and shall be responsible for managing and directing the Company's CPNI compliance efforts, included but not limited to providing interpretive guidance (with the advice and consent of outside counsel as necessary), employee training programs, situational responses, conducting annual program reviews, updating Company CPNI programs, and making any filings required by law.

B|1.3. Questions regarding the interpretation of the CPNI Rules, the provisions of this Manual, or a proposed use or disclosure of CPNI under circumstances not covered by this Manual must be referred to the Compliance Officer. The Compliance Officer will then review the question and, if necessary, seek the advice of outside counsel. Once a determination is made, the Compliance officer will circulate the question and the answer to all employees, and will also update the Q&A section of this Manual.

B|1.4. Company employees are prohibited from engaging in any activity involving any use of or access to CPNI that is not addressed by this Manual unless and until the Compliance Officer has provided guidance and direction concerning such activity to all employees.

B|1.5. Unauthorized use of or access to CPNI by Company employees will result in appropriate disciplinary action in accordance with established Company disciplinary policies and practices, including any factors indicating that such access or use was inadvertent. Unauthorized use of or access to CPNI shall be considered a serious offense, and may result in suspension or termination of employment in appropriate cases. Under all circumstances, Company personnel that improperly uses or discloses CPNI will be required to undergo remedial training as necessary to ensure future compliance.

B|1.6. The Company will notify the FCC in writing within five business days if an opt-out mechanism fails, and the failure is considered more than mere anomaly. The notice must include:

B|1.6.1. The Company's name, a description of the applicable opt-out mechanism, the nature of the problem, how and when the problem was solved (or if no solution has yet been identified, the status of the Company's efforts to solve the problem, and when the Company expects to implement a solution), whether relevant state commissions must be notified, and if so whether those commissions have taken any action, a copy of the notice provided to Customers, and contact information.

B|1.6.2. The notice must be provided to the FCC even if the Company offers consumers alternate opt-out mechanisms.

B|1.7. On or before March 1st of each year, the Compliance Officer or other authorized officer of the

Company will sign and file with the Federal Communications Commission Enforcement Bureau a Compliance Certificate and accompanying statement (see Exhibit 1.9) that:

B|1.7.1. Confirms that the Company has established CPNI operating procedures that are adequate to ensure compliance with the CPNI rules.

B|1.7.2. Explains any actions taken against data brokers, i.e., proceedings instituted or petitions filed by the Company in court or with a state or federal commission.

B|1.7.3. Summarizes customer complaints received in the past year concerning unauthorized release of CPNI by the Company. This summary must give the number of complaints received, categorized by event type (e.g., unauthorized employee access, unauthorized disclosure by Company employees, and unauthorized online access to CPNI by third parties.

B|1.7.4. Reports any information the Company has concerning pretexting techniques used in attempts to access CPNI, and the steps the Company has taken to thwart such efforts.

B|1.7.5. This annual filing will be made with the FCC's Enforcement Bureau on or before March 1 in EB Docket No. 06-36, for data pertaining to the previous calendar year.

B|1.8. The Company will review and revise these procedures on a continuing basis to address weaknesses and ensure compliance with applicable FCC regulations.

B|2. Recordkeeping.

B|2.1. The Company will create and, for a period of not less than one year, maintain clearly identified records:

B|2.1.1. Of sales and marketing campaigns conducted by the Company or an Affiliate that use CPNI, including a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign.

B|2.1.2. Cases in which the Company or an Affiliate disclosed CPNI to a third party, or allowed a third party to access CPNI, including where applicable a description of the marketing campaign, the specific CPNI used in the campaign, and the products and services that were offered as a part of the campaign

B|2.2. The Company will maintain records of Customer approval of CPNI use, as well as notices required by FCC regulations, for a minimum of one year from the date the approval or notice is given in a readily-available location that is consulted on an as-needed basis.

B|2.3. The Company will maintain separate files containing court orders concerning CPNI.

B|3. Authentication and Procedural Safeguards.

B|3.1. The Company will implement and maintain measures reasonably likely to identify and protect against unauthorized efforts to access CPNI.

B|3.2. The Company will implement and maintain processes to verify the identity of a Customer before disclosing CPNI online, during a Customer-initiated telephone call, or a Customer visit to a Company facility.

B|3.3. The Company will only disclose "Call Detail" CPNI6 during a Customer-initiated telephone call if the Customer first provides the correct password for the account without being asked for readily available biographical or account information7.

B|3.3.1. If the Customer does not provide the correct password for the account, or does not wish to go through the process required to create a password, the Company may only disclose CPNI for the account by sending it to the address listed in the Company's account records, or by calling the Customer at the phone number listed in the account records. Under no circumstances should the number of the caller be relied on for this purpose.

B|3.3.2. If the Customer provides the correct account password during a customer-initiated

telephone call without being asked for readily available biographical or account information, then the Company is permitted to discuss CPNI that is provided by the customer during the call. CPNI that is in the Company's records but not provided by the caller, even if the correct account password has been provided, may not be discussed during a customer-initiated telephone call.

B|3.3.3. If a Customer requests CPNI that is not considered Call Detail CPNI, then the Company not required to obtain the account password from the caller, but must nevertheless verify that the caller is the customer. In such cases, the Customer is not required to setup a password, but the Company must provide the Customer the option to do so.

B|3.4. Prior to allowing online access to CPNI, the Company must authenticate a Customer without the use of Readily Available Biographical Information, or Account Information.

B|3.4.1. Authenticated online customers may only access CPNI with the correct account password.

B|3.4.2. As with telephone inquiries, online customers must provide the account password without being prompted for Readily Available Biographical Information, or Account Information. The Company may choose to block access to a Customer's account after repeated unsuccessful attempts to log into that account.

B|3.5. Customers who visit the offices of the company and wish to examine CPNI for their account must first provide a valid photo ID, and the information on the ID must match the account records. Visiting customers may not access or review Call Detail CPNI.

B|3.6. As noted above, customers seeking access to CPNI must be authenticated without the use of Readily Available Biographical or Account Information.

B|3.6.1. So long as the requirements of the CPNI Rules and this Manual are met, the Company may establish account passwords using one a combination of reasonable methods, including but not limited to:

B|3.6.2. Assigning a randomly generated alpha-numeric password to each account.

B|3.6.3. Assigning a randomly generated personal identification number ("PIN") to each account, and allowing the customer to create an account password by providing the correct PIN.

B|3.6.4. A combination of either of the foregoing with a "shared secret" form of authentication.

B|3.6.5. The Company may supply the PIN to the Customer by a Company-originated voicemail or text message to the Telephone Number of Record, or by sending it to an Address of Record so as to reasonably ensure that it is delivered to the intended party.

B|3.6.6. The Company is not required to create new passwords for customers who already have a password, even if the password uses Readily Available Biographical Information.

B|3.6.7. The Company may not, however, prompt a customer for Readily Available Biographical or Account Information as a primary or secondary method of customer authentication.

B|3.6.8. The Company may also create a "back-up," or secondary authentication method in the event of a lost or forgotten password. As in all other cases, however, the secondary authentication method may not prompt the Customer for Readily Available Biographical or Account Information.

B|3.6.9. If a customer cannot provide the correct password or the correct response for the secondary authentication method, the customer must establish a new password.

B|3.7. The Company must promptly notify a customer whenever a password, customer response to a secondary authentication method for lost or forgotten passwords, online account, or Address of Record is created or changed.

B|3.7.1. Notification may be given by a Company-originated voicemail or text message to the telephone number listed in the account records, or by mail to the address listed in the account records. The notification must not however, reveal or be sent using the new account information.

B|3.7.2. A change of address should be mailed to the former address, rather than the new address.

B|3.7.3. Notification is not required when the Customer initiates service, or establishes a password as a step in the service initiation process.

B|3.8. The Company may bind itself contractually to authentication regimes other than those described in this Manual for services provided to business Customers that have both a dedicated account representative and a contract that specifically addresses the Company's protection of CPNI.

B|4. Notification of CPNI Security Breaches.

B|4.1. The Company will take reasonable steps to protect CPNI databases from unauthorized third party access.

B|4.2. The Company must notify law enforcement whenever a person accesses, uses, or discloses CPNI without authorization or, if authorized, in a manner that exceeds the scope of such authorization (a "CPNI Breach").

B|4.3. The Company may not, however, notify customers or publicly disclose a CPNI Breach, either voluntarily or pursuant to state or local law or these rules, until it has notified appropriate law enforcement entities.

B|4.3.1. As soon as practicable, but in no event more than seven (7) days from the date the Company reasonably determines that a CPNI Breach has occurred, the Company must notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through the central reporting facility maintained by the FCC at http://www.fcc.gov/eb/cpni (the "Federal Notice").

B|4.3.2. If the Company desires to notify its customers or a class of customers contemporaneously with the Federal Notice, it must include a statement to that effect in the Federal Notice.

B|4.4. Subject to Paragraph 4.5, the Company must wait at least seven (7) full business days from the date of the Federal Notice to notify customers or publicly disclose a CPNI Breach, even if earlier disclosure is required by applicable state law; provided, however, that:

B|4.4.1. If the Company believes that there is an extraordinarily urgent need to notify a subgroup of affected customers before the expiration of the seven (7) day period in order to avoid immediate and irreparable harm, it may proceed with such customer notifications after consulting with and receiving the approval of the relevant investigating agency (the "Investigating Agency").

B|4.4.2. The Company shall cooperate with any request made by the Investigating Agency for the purpose of minimizing any adverse effects the notification could have on the Investigating Agency's investigation.

B|4.5. If the Investigating Agency concludes that public disclosure or notice to customers would compromise national security or impede an ongoing or potential criminal investigation, the

Investigating Agency may direct the Company to refrain from notifying customers or publicly disclosing the CPNI Breach.

B|4.5.1. Initially, the Investigating Agency may require the company to delay notification and disclosure for up to thirty (30) days.

B|4.5.2. The Investigating Agency may extend the delay, however, if reasonably necessary in the judgment of the Investigating Agency in the interest of national security or a criminal investigation, and in such cases the Company must wait for authorization from the Investigating Agency before notifying customers or publicly disclosing the CPNI Breach.

B|4.5.3. Investigating Agency directives must be given in writing, and all such directives will be logged with the same reporting facility that maintains records of notifications filed by other carriers.

B|4.6. After the Company has completed steps described in Paragraph 4.5, the Company is required to deliver notice of the CPNI breach to affected customers.

B|4.7. The Company must maintain electronic or tangible records of CPNI Breaches, notifications given to the USSS and the FBI, and notifications given to customers. These records must include, if available, the dates the CPNI Breach was discovered, the dates required notifications were given, a detailed description of the CPNI that was accessed, used, or disclosed as a result of the CPNI Breach, and the circumstances underlying the CPNI Breach. The Company must retain these records for a minimum of two (2) years from the date the Company notifies the USSS and FBI of the applicable CPNI Breach.

Appendix 1

Marketing Services and Customer Consent
(Additional Discussion)

USING CPNI FOR MARKETING - THE "TOTAL SERVICE APPROACH"
The FCC has adopted an approach to safeguard CPNI based on the services to which a customer subscribes. This is called the "total service approach." This approach permits the use of CPNI for marketing of telecommunication services, depending on the "existing service relationship" between a customer and the carrier.

Telecommunication services are segmented into three distinct silos - local, long distance and wireless services. A carrier is allowed to use the customer's CPNI for marketing purposes within the particular silo, to which the customer already subscribes. The carrier may use that information to market products and services that are directly related to those particular services, but only those services.
For example: if a customer subscribes to local exchange service but not to long distance service, the company could use any existing information about that customer to market new products, service enhancements, or other improvements related to the local exchange service, without any additional customer approval. However, in order to use CPNI to market a service that is outside the customer's existing service relationship, in this example the long distance service, the company is required to obtain express customer approval to use this information.
When a company wants to use a customer's CPNI to market services outside of the "existing service relationship", the company will need the customer's consent to do so.

"OPT-IN" & "OPT-OUT" NOTIFICATIONS AND CONSENTS

The FCC has established specific rules governing customer notifications and consents. Two approaches are available for us by the Company: "opt-in" and "opt-out."

"**Opt-in**" consent is required before there can be any CPNI use or disclosure with respect to marketing other than "communications-related services". This approach requires express customer consent that is obtained after giving customers actual notification of the intended use of their CPNI. The consent must be affirmative – not passive – and must be manifested by a customer signature, either actual or electronic. "Opt-in" consent is a "tell us we can use" approach, such as no response by the customer means that the CPNI may not be used. In other words, **"silence is NOT acceptance**". (Opting-in" is the more difficult approach because the potential that CPNI may be more widely disseminated and used by those providing "non-communications related services," thereby justifying the solicitation and receipt of written consents from customers.) Currently, the Company does not use CPNI for any marketing requiring an "opt-in" consent.
"**Opt-out**" consent solicited by the Company, is obtained before the Company, or an affiliate uses customer CPNI to market "communications-related services." Individual customers are notified of the intended use of their CPNI and are given the opportunity to indicate that the Company may not use their CPNI. Any failure by the customers to respond to the Company's CPNI notification by "opting-out" constitutes a knowing consent to the intended use of the CPNI. ("Opting-out" is less onerous than "opting-in" because it is a "tell me if we can't use the CPNI", such that no response on the part of the customer constitutes a "known consent" to the intended use.) In other words, **silence is acceptance**.

Opt-out notifications will be written and delivered by bill insert to affected customers. The notice will provide information sufficient to enable customers to make informed decisions as to whether to permit the Company to use, disclose, or permit access to the their CPNI. The notice will inform customers of their ability to "opt-out" at no additional cost and at any time.

After notice is delivered to customers, the Company will wait at least 30 days before assuming consent. (The 30-day timeframe begins on the third day after the notice is mailed.)

A copy of the sample "Opt-Out" notice is listed in the Attachments to this policy manual. If the Company decided to use this approach to marketing, an "opt-out" refresher notice must be mailed every two years.

Appendix 2

CUSTOMER NOTICE: OPT-OUT CONSENT
(Included with the first statement for new customers; annually in all customer statements)
IMPORTANT CUSTOMER NOTICE

AB&T Telecom LLC ("AB&T Telecom") employs comprehensive safeguards to protect the privacy of your information under federal law. The Federal Communications Commission ("FCC") requires AB&T Telecom to notify all customers of their additional rights to restrict the use of their Customer Proprietary Network Information ("CPNI").

What is CPNI?
Simply stated, CPNI is information that relates to your use of telecommunications services, such as the technical configuration, type of use, destination, and amount you use your services, including the information contained on your bill. Examples of CPNI include information about which services you purchase, the amount of your long distance bill, or certain details concerning your phone calls.
CPNI does not, however, include your published directory information or any information that is already in the public domain, such as your name, address or published telephone number.

Permitted Use of CPNI by AB&T Telecom Without Your Permission
CPNI can be used for certain purposes without your permission. For example, CPNI may be used to offer you new or enhanced services, such as speed dialing, call forwarding or caller ID, that are related to the services you currently purchase, or to respond to your inquiry regarding the services you currently use. CPNI may also be used without your permission for purposes related to billing and collection, repair and maintenance, installation of inside wiring, to protect the property of AB&T Telecom and others, and to prevent fraud.

Opt-Out Consent for Marketing Communication
Telecommunications service providers such as AB&T Telecom are required to notify you that you have the right to "opt-out" from the use of your CPNI, and provide you with an opportunity to make that choice. Consequently, we are sending you this notification because from time-to-time your CPNI may be useful to us in identifying and designing new products and services for you and other AB&T Telecom customers, and letting you know about those services when they become available.

You need to respond this notice if you do not wish to give us permission to use your information in our service development and marketing plans, in which case you need to respond to this notice within 30 days of the date of this notice. Otherwise, your consent will remain valid until we receive written notice from you withdrawing your consent.

And whether you opt-out or later withdraw your consent, it will not affect how we provision your services.

Appendix 3

CUSTOMER NOTICE: FCC AUTHENTICATON REQUIREMENTS
(Included with the first statement for new customers; annually in all customer statements)

FCC RULES GOVERNING ACCESS TO YOUR ACCOUNT

The Federal Communications Commission has adopted privacy rules requiring telephone, wireless, and VoIP providers to implement additional safeguards for the purpose of preventing unauthorized access to customer telephone records. Among other things, these safeguards the release of "call detail information" during a telephone call initiated by a customer unless the customer provides a password.

Accordingly, AB&T Telecom LLC uses certain tools to confirm the identity of customers before releasing certain kinds of information pertaining to the details of calls or your account. When you contact AB&T Telecom, you may be asked to go through the process of creating a password in order to access your account on-line, or obtain information concerning your account.

We are writing to encourage you to set up a password for your account, if you haven't already, to ensure that we can provide you with the information and service you expect from us.

While the password set-up process may seem cumbersome to some, it is designed to protect your information from anyone who might try to access your account without your authorization. And, If you haven't created a password for your account, or can't provide it to use when we ask for it, we will be required to either mail information to your "address of record," or call back at the "telephone number of record."

If you have questions, please contact us at [customer support phone number(s)]. Thank you for your cooperation. It is a pleasure to serve you.

APPENDIX 4

CUSTOMER CONSENT: ONE-TIME CPNI USE

VERBAL NOTIFICATION OF CUSTOMER RIGHTS FOR LIMITED USE OF CPNI FOR THE DURATION OF THE CALL

“Under federal and state law, you have the right - and AB&T Telecom has a duty – to protect the confidentiality of certain information concerning your account and your use of our services that we collect in the normal course of providing services to you. Examples include information about how many telecommunication services you have, which services and features you use, how many calls you make, what time of day you make most calls, and the related billing for these services.

“With your permission, I can obtain access to and use your information for the duration of this call to inform you of services provided by the company or one of its affiliates. Do I have your permission use that information during this call for that purpose?

“Your decision to grant or deny permission will not affect your services, but may affect my ability to answer questions and provide information during this call.

“AB&T Telecom respects your privacy, and does not sell, trade or share your confidential information with unaffiliated third parties without your approval, except as required by law.”

Appendix 5

WRITTEN CUSTOMER AUTHORIZATION FOR RELEASE OF CPNI

I authorize AB&T Telecom LLC to release any information in its possession protected under the Federal Communications Commission CPNI rules (the "Rules"). I have read the customer notification information and understand my rights under the Rules. I also understand that I may limit or revoke this authorization at any time by providing the required notice to AB&T Telecom LLC. This authorization will remain effective until I revoke it.

Customer Name: _____
Address: _____
Phone #: _____
Date: _____
Signature: _____
Please return this authorization to our business office at:

AB&T Telecom LLC
9841 Broken land Parkway #118
Columbia, MD 21046

Appendix 6

TELEPHONIC CUSTOMER AUTHORIZATION FOR RELEASE OF CPNI (SCRIPT)

To be read by employee to customer via telephone. If customer has questions, employee may need to refer to the customer Notification Regarding CPNI section. This information must be verified by either an independent third party, such as audio-taping, independent verification company or authorized company employee.

"I understand that you are interested in giving AB&T Telecom permission to use your customer proprietary network information, information that may be used to market new services that AB&T Telecom believes will interest you.

If so, I'll need you to listen to verbally agree with a brief statement which I'll read to you, after which my supervisor and I will sign a copy of the statement indicating confirming your consent. Also, this conversation is being recorded for verification purposes of later verification, either by us or by a third party.
If you have no further questions about the information or how it can be used, please listen to the following statement:

If the customer agrees, the employee should read the following statement, ask the customer to agree with the statement, and the employee and the employee's supervisor should then sign the statement.

I authorize AB&T Telecom LLC to use any information in its possession protected under FCC CPNI rules. I understand my rights under Federal CPNI rules. I understand that I may limit or revoke this authorization at any time upon proper notice to AB&T Telecom LLC

Customer Information:
Name: _____ Phone: _____

Address: _____ Date: _____

_____ _____
Employee Supervisor

Appendix 7

Annual Compliance Certification

Annual 47 C.F.R. & 64.2009(e) CPNI Certification for 2015 EB Docket 06-36
Date filed: March 2, 2015

Name of company covered by this certification: AB&T Telecom, LLC.
9841 Broken Land Parkway #118, Columbia, MD 21046
Form 499 Filer ID: 830402

Name of signatory: Emmet Tydings
Title of signatory: President

I, Emmet Tydings, certify that I am an officer AB&T Telecom LLC ("Company"), and that acting as an agent of the company, I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with CPNI rules promulgated by the Federal Communications Commission ("Commission") and set forth in 47 CFR, Chapter I, Part 64, Subpart U (the "CPNI Rules").

Actions Against Data Brokers
The Company **has not** instituted proceedings, filed petitions, or initiated comparable action before a state commission, a court system, or the Commission against data brokers in the past year.

Customer Complaints
The Company **has not** received customer complaints in the past year concerning the unauthorized release of CPNI.

Explanation of Operating Procedures
In accordance with the requirements set forth in 47 CFR §64.2009(e), attached to this certificate is a statement explaining how the Company's operating procedures ensure that the Company is in compliance with the requirements set forth in the CPNI Rules.

Emmet Tydings,
President

Annual 47 C.F.R. 64.2009(e) CPNI Certification EB Docket 06-36
Statement Concerning CPNI Operating Procedures
(submitted Pursuant to 47 CFR §64.2009(e))

AB&T Telecom LLC 9841 Broken Land Parkway #118, Columbia, MD 21046
To ensure compliance with the provisions of 47 CFR, Chapter I, Part 64, Subpart U (the "CPNI Rules"), the Company has adopted practices that are consistent with the highly sensitive nature of CPNI, the text and purpose of the CPNI Rules, and the limited use of CPNI by the Company. These practices include:

- Educating Company personnel regarding authorized and unauthorized use of CPNI, circumstances under which CPNI may be shared and procedures that must be followed, and protecting CPNI from inadvertent or accidental disclosure to unauthorized third parties.

This instruction is intended to ensure that Company personnel: (a) know what constitutes CPNI; (b) understand and participate in the Company's efforts to protect CPNI; (c) know when they are, and are not, authorized to use CPNI; (d) confirm that each customer has consented to the use of CPNI for marketing purposes in accordance with Company procedures before using CPNI for such purposes; and (e) are aware of and comply with record keeping requirements applicable to customer complaints concerning CPNI, and the use of CPNI for marketing purposes.

- Taking appropriate disciplinary action in cases where Company personnel fail to follow such practices.
- Using authentication techniques that do not incorporate CPNI or other readily available biographical information to identify customers before permitting online access to, or communicating verbally with regard to a customer account. The Company may negotiate alternative authentication procedures for business customers that have both a dedicated account representative and a contract that specifically addresses the protection of CPNI.
- Except as otherwise required by law, prohibiting the disclosure of CPNI (a) to third parties other than Company Affiliates, and (b) to an Affiliate of the Company, unless the relevant customer has subscribed to a service that is provided by such Affiliate.
- The Company will electronically report CPNI breaches within 7 days to the US Secret Service and the FBI through the designated central reporting facility at https://www.cpnireporting.gov. Following electronic notification to the designated central reporting facility, an affected customer will be promptly notified by mail unless the Company is otherwise instructed by law enforcement.
- Prohibiting the use of CPNI for the purpose of marketing new categories of service to existing customers without first obtaining such customer's consent to the use of CPNI for
- such purposes.
- Maintaining records of the sales and marketing campaigns executed by the Company and its Affiliates that use CPNI.
- Restricting decisions regarding the use and disclosure of CPNI to Company management, and requiring Company management oversee opt-in, opt-out, and other customer approval and customer notice processes.
- Promptly notifying customers by mail whenever a password, customer response to a backup means of authentication for lost or stolen passwords, online account, or address of record is created or changed. This notification is not provided when the customer initiates service, including the selection of a

password at service initiation.

- Employing reasonable measures to discover and protect against unauthorized access to CPNI.

Appendix 8

CPNI RULES
47 CFR Part 64-- MISCELLANEOUS RULES RELATING TO COMMON CARRIERS Subpart U -- customer Proprietary Network Information
§64.2001 Basis and Purpose.

(a) Basis. These rules in this subpart are issued pursuant to the Communications Act of 1934, as amended.

(b) Purpose. The purpose of these rules in this subpart is to implement section 222 of the Communications Act of 1934, as amended, 47 U.S.C. 222.

§64.2003 Definitions.
Terms used in this subpart have the following meanings:

(a) Account information. Account information" is information that is specifically connected to the customer's service relationship with the carrier, including such things as an account number or any component thereof, the telephone number associated with the account, or the bill's amount.

(b) Address of record. An "address of record," whether postal or electronic, is an address that the carrier has associated with the customer's account for at least 30 days.

(c) Affiliate. An affiliate is an entity that directly or indirectly owns or controls, is owned or controlled by, or is under common ownership or control with, another entity.

(d) Call detail information. Any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.

(e) Communications-related services. The term "communications-related services" means telecommunications services, information services typically provided by telecommunications carriers and services related to the provision or maintenance of customer premises equipment.

(f) customer. A customer of a telecommunications carrier is a person or entity to which the telecommunications carrier is currently providing service.

(g) customer proprietary network information (CPNI). customer proprietary network information (CPNI) is:

(1) information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the customer-carrier relationship;

(2) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier. customer proprietary network information

does not include customer list information.

(h) customer premises equipment (CPE). customer premises equipment (CPE) is equipment employed on the premises of a person (other than a carrier) to originate, route, or terminate telecommunications.

(i) Information services typically provided by telecommunications carriers. The phrase "information service typically provided by telecommunications carriers" means only those information services that are typically provided by telecommunications carrier, such as Internet access or voice mail services that offer a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications and includes electronic publishing, but does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service.

(j) Local exchange carrier (LEC). A local exchange carrier (LEC) is any person that is engaged in the provision of telephone exchange service or exchange access. For purposes of this subpart, such term does not include a person insofar as such person is engaged in the provision of commercial mobile service under 47 U.S.C. 332(c).

(k) Opt-In Approval. The term "opt-in approval" refers to a method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. This approval method requires that the carrier obtain from the customer affirmative, express consent allowing the requested CPNI usage, disclosure or access after the customer is provided appropriate notifications of the carrier's request consistent with the requirements set forth in this subpart.

(l) Opt-Out Approval. The term "opt-out approval" refers to a method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. Under this approval method, a customer is deemed to have consented to the use, disclosure, or access to the customer's CPNI if the customer has failed to object thereto within the waiting period after the customer is provided appropriate notification of the carrier's request for consent.

(m) Readily available biographical information. "Readily available biographical information" is information drawn from the customer's life history and includes such things as the customer's social security number, or the last four digits of that number; mother's maiden name; home address; or date of birth.

(n) **customer list information (SLI)**. customer list information (SLI) is any information:

(1) identifying the listed names of customers of a carrier and such customers telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications;

(2) that the carrier or an affiliate has published, caused to be published, or accepted for publication in any directory format.

(o) **Telecommunications carrier**. A telecommunications carrier is any provider of telecommunications services, except that such term does not include aggregators of telecommunications services (as defined in 47 U.S.C. 226(a)(2)).

(p) **Telecommunications service**. The term "telecommunications service" has the same meaning given to such term in section 3(46) of the Communications Act of 1934, as amended, 47 U.S.C. 153(46).

(q) **Telephone number of record**. The telephone number associated with the underlying service, not the telephone number supplied as a customer's "contact information."

(r) **Valid photo ID**. A "valid photo ID" is a government-issued means of personal identification with a photograph such as a driver's license, passport, or comparable ID that is not expired.

§64.2005 Use of customer Proprietary Network Information Without customer Approval

(a) Any telecommunications carrier may use, disclose, or permit access to CPNI for the purpose of providing or marketing service offerings among the categories of service (i.e., local, interexchange, and CMRS) to which the customer already subscribes from the same carrier, without customer approval.

(1) If a telecommunications carrier provides different categories of service and a customer subscribes to more than one category of service offered by the carrier, the carrier is permitted to share CPNI among the carrier's affiliated entities that provide a service offering to the customer.

(2) If a telecommunications carrier provides different categories of service, but a customer does not subscribe to more than one offering by the carrier, the carrier is not permitted to share CPNI among the carrier's affiliated entities.

(b) A telecommunications carrier may not use, disclose, or permit access to CPNI to market to a customer service offerings that are within a category of service to which the customer does not already subscribe from that carrier, unless the carrier has customer approval to do so, except as described in paragraph (c) of this section.

(1) A telecommunications carrier may use, disclose, or permit access to CPNI derived from its provision of local service, interexchange service, or CMRS, without customer approval, for the provision of CPE and information services, including call answering, voice mail or messaging, voice storage and retrieval services, fax store and forward, and Internet access services. (2) A telecommunications carrier may not use, disclose, or permit access to CPNI to identify or track customers that call competing service providers. For example, a local exchange carrier may not use local service CPNI to track all customers that call local service competitors.

(c) A telecommunications carrier may use, disclose, or permit access to CPNI, without customer approval, as described in this subparagraph.

(1) A telecommunications carrier may use, disclose, or permit access to CPNI, without customer approval, in its provision of inside wiring installation, maintenance, and repair services.

(2) CMRS providers may use, disclose, or permit access to CPNI for the purpose of conducting research on the health effects of CMRS.

(3) LECs and CMRS providers and entities that provide interconnected VoIP service may use CPNI, without customer approval, to market services formerly known as adjunct-to-basic services, such as, but not limited to, speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller I.D., call forwarding, and certain Centrex features.

(d) A telecommunications carrier may use, disclose, or permit access to CPNI to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive or unlawful use of, or subscription to, such services.

§64.2007 Approval required for Use of CPNI

(a) A telecommunications carrier may obtain approval through written, oral or electronic methods.

(1) A telecommunications carrier relying on oral approval shall bear the burden of demonstrating that such approval has been given in compliance with the Commission's rules.

(2) Approval or disapproval to use, disclose, or permit access to a customer's CPNI obtained by a telecommunications carrier must remain in effect until the customer revokes or limits such approval or disapproval.

(3) A telecommunications carrier must maintain records of approval, whether oral, written or electronic, for at least one year.

(b) Use of Opt-out and Opt-In Approval Processes. A telecommunications carrier may, subject to opt-out approval or opt-in approval, use its customer's individually identifiable CPNI for the purpose of marketing communications-related services to that customer. A telecommunications carrier may, subject to opt-out approval or opt-in approval, disclose its customer's individually identifiable CPNI, for the purpose of marketing communications-related services to that customer, to its agents and its affiliates that provide communications-related services. A telecommunications carrier may also permit such persons or entities to obtain access to such CPNI for such purposes. Except for use and disclosure of CPNI that is permitted without customer approval under section Sec. 64.2005, or that is described in this paragraph, or as otherwise provided in section 222 of the Communications Act of 1934, as amended, a telecommunications carrier may only use, disclose, or permit access to its customer's individually identifiable CPNI subject to opt-in approval.

(1) Joint Venture/Contractor Safeguards. A telecommunications carrier that discloses or provides access to independent contractors shall enter into confidentiality agreements with independent contractors or joint venture partners that comply with the following requirements. The confidentiality agreement shall:

(i) Require that the independent contractor or joint venture partner use the CPNI only for the purpose of marketing or providing the communications-related services for which that CPNI has been provided;

(ii) Disallow the independent contractor or joint venture partner from using, allowing access to, or disclosing the CPNI to any other party, unless required to make such disclosures under force of law; and

(iii) Require that the independent contractor or joint venture partner have appropriate protections in place to ensure the ongoing confidentiality of consumer's CPNI.

(2) Except for use and disclosure of CPNI that is permitted without customer approval under section 64.2005 or that is described in paragraph (b)(1) of this section, or as otherwise provided in Section 222 of the Communications Act of 1934, as amended, a telecommunications carrier may only use, disclose, or permit access to its customer's individually identifiable CPNI subject to opt-in approval

§64.2008 Notice required for use of CPNI

(a) Notification generally:

(1) Prior to any solicitation for customer approval, a telecommunications carrier must provide a one-time notification to the customer of the customer's right to restrict use of, disclosure of, and access to that customers CPNI.

(2) A telecommunications carrier must maintain records of notification, whether oral or electronic, for at least one year.

(b) Individual notice to customers must be provided when soliciting approval to use, disclose or permit access to customer's CPNI.

(c) Content of notice. customer notification must provide sufficient information to enable the customer to make an informed decision as to whether to permit a carrier to use, disclose or permit access to the customer's CPNI.

(1) The notification must state that the customer has a right, and the carrier a duty, under federal law, to protect the confidentiality of CPNI.

(2) The notification must specify the types of information that constitute CPNI and the specific entities that will receive the CPNI, describe the purposes for which CPNI will be used, and inform the customer of his or her right to disapprove those uses and deny or withdraw access to CPNI at any time.

(3) The notification must advise the customer of the precise steps the customer must take in order to grant or deny access to CPNI and must clearly state that a denial of approval will not affect the provision of any services to which the customer subscribes. However, carriers may provide a brief statement, in clear and neutral language, describing consequences directly resulting from the lack of access to CPNI.

(4) The notification must be comprehensible and not be misleading.

(5) If written notification is provided, the notice must be clearly legible, use sufficiently large type, and be placed in an area so as to be readily apparent to a customer.

(6) If any portion of a notification is translated into another language, then all portions of the notification must be translated into that language.

(7) A carrier may state in the notification that the customer's approval to use CPNI may enhance the carrier's ability to offer products and services tailored to the customer's needs. A carrier also may state in the notification that it may be compelled to disclose CPNI to any person upon affirmative written request by the customer.

(8) A carrier may not include in the notification any statement attempting to encourage a customer to freeze third-party access to CPNI.

(9) The notification must state that any approval, or denial of approval for the use of CPNI outside of the service to which the customer already subscribes from that carrier is valid until the customer affirmatively revokes or limits such approval or denial.

(10) A telecommunications carrier's solicitation for approval must be proximate to the notification of a customer's CPNI rights.

(d) Notice Requirements Specific to Opt-Out . A telecommunications carrier ,must provide notifications to obtain opt-out approval through electronic or written methods, but not by oral communication (except as provided in paragraph (f) of this section). The contents of any such notification must comply with the requirements of paragraph (c) of this section.

(1) the Company must wait a 30 day minimum period of time after giving customers notice and an opportunity to opt-out before assuming customer approval to use, disclose or permit access to CPNI. A carrier may, in its discretion, provide for a longer period. the Company must notify customers as to the applicable waiting period for a response before approval is assumed.

(i) In the case of an electronic form of notification, the waiting period shall begin to run from the date on which the notification was sent; and

(ii) In the case of notification, by mail, the waiting period shall begin to run on the third day following the date that the notification was mailed.

(2) the Company using the opt-out mechanism must provide notices to their customers every two years.

(3) Telecommunications carriers that use e-mail to provide opt-out notices must comply with the following requirements in addition to the requirements generally applicable to notifications:

(i) the Company must obtain express, verifiable, prior approval from consumers to send notices via e-mail regarding their service in general, or CPNI in particular;

(ii) the Company must allow customers to reply directly to e-mails containing CPNI notices in order to opt-out;

(iii) Opt-out e-mail notices that are returned to the carrier as undeliverable must be sent to the customer in another form before carriers may consider the customer to have received notice;

(iv) the Company that use e-mail to send CPNI notices must ensure that the subject line of the message clearly and accurately identifies the subject matter of the e-mail and;

(v) Telecommunication carriers must make available to every customer a method to opt-out that is of no additional cost to the customer and that is available 24 hours a day, seven days a week. the Company may satisfy this requirement through a combination of methods, so long as all customer have the ability to opt-out at no cost and are able to effectuate that choice whenever they choose.

(e) Notice Requirements Specific to Opt-In. A telecommunications carrier may provide notification to obtain opt-in approval through oral, written or electronic methods. The contents of any such notification must comply with the requirements of paragraph (c) of this section.

(f) Notice Requirements Specific to One Time Use of CPNI.

(1) the Company may use oral notice to obtain limited, one-time use of CPNI for inbound and outbound customer telephone contacts for the duration of the call, regardless of whether carriers use opt-out or opt-in approval based on the nature of the contact.

(2) The contents of any such notification must comply with the requirements of paragraph (c) of this section. except that telecommunications carrier may omit any of the following notices provisions if

not relevant to the limited use for which the carrier seeks CPNI.

(i) the Company need not advise customers that if they have opted-out previously, no action is needed to maintain the opt-out election.

(ii) the Company need not advise customers that they may share CPNI with their affiliates or third parties, and need not name those entities, if the limited CPNI usage will not result in use by or disclosure to, an affiliate or third party.

(iii)the Company need not disclose the means by which a customer can deny or withdraw future access to CPNI, so long as carriers explain to customers that the scope of the approval the carrier seeks is limited to one-time use; and
(iv) the Company may omit disclosure of the precise steps a customer must take in order to grant or deny access to CPNI, as long as the carrier clearly communicates that the customer can deny access to his CPNI for the call.

§64.2009 Safeguards Required for Use of CPNI

(a) Telecommunications carriers must implement a system by which that status of a customer's CPNI approval can be clearly established prior to the use of CPNI.

(b) Telecommunications carriers must train their personnel as to when they are and are not authorized to use CPNI, and carriers must have an express disciplinary process in place.

(c) Telecommunications carriers shall maintain a record, electronically or in some other manner of their own and their affiliate's sales and marketing campaigns that use their customers' CPNI. All carriers shall maintain a record of all instances where CPNI was disclosed or provided to third parties or where third parties were allowed access to CPNI. The record must include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign. the Company shall retain the record for a minimum of one year.

(d) Telecommunications carriers must establish a supervisory review process regarding carrier compliance with the rules in this subpart for outbound marketing situations and maintain records of carrier compliance for a minimum period of one year. Specifically, sales personnel must obtain supervisory approval of any proposed outbound marketing request.

(e) A telecommunications carrier must have an officer, as an agent of the carrier, sign and file with the Commission a compliance certificate on an annual basis. The officer must state in the certification that he or she has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the rules in this subpart. The carrier must provide a statement accompanying the certificate explaining how its operating procedures ensure that it is or is not in compliance with the rules in this subpart. In addition, the carrier must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. This filing must be made annually with the Enforcement Bureau on or before March 1 in EB Docket No. 06-36, for data pertaining to the previous calendar year.
(f) the Company must provide written notice within 5 business days to the Commission of any instance where the opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly.

(1) The notice shall be in the form of a letter and shall include the carrier's name, a description of the opt-out mechanism(s) used, the problem(s) experienced, the remedy proposed and when it will be/was implemented. Whether the relevant state commission(s) have been notified and whether it has taken any action, a copy of the notice provided to customers, and contact information.

(2) Such notice must be submitted even if the carrier offers other methods by which consumers may opt-out.

Sec. 64.2010 Safeguards on the disclosure of customer proprietary network information.

(a) Safeguarding CPNI. Telecommunications carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Telecommunications carriers must properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, online account access, or an in-store visit.

(b) Telephone access to CPNI. Telecommunications carriers may only disclose call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides the carrier with a password, as described in paragraph (e) of this section, that is not prompted by the carrier asking for readily available biographical information, or account information. If the customer does not provide a password, the telecommunications carrier may only disclose call detail information by sending it to the customer's address of record, or by calling the customer at the telephone number of record. If the customer is able to provide call detail information to the telecommunications carrier during a customer-initiated call without the telecommunications carrier's assistance, then the telecommunications carrier is permitted to discuss the call detail information provided by the customer.

(c) Online access to CPNI. A telecommunications carrier must authenticate a customer without the use of readily available biographical information, or account information, prior to allowing the customer online access to CPNI related to a telecommunications service account. Once authenticated, the customer may only obtain online access to CPNI related to a telecommunications service account through a password, as described in paragraph (e) of this section, that is not prompted by the carrier asking for readily available biographical information, or account information.

(d) In-store access to CPNI. A telecommunications carrier may disclose CPNI to a customer who, at a carrier's retail location, first presents to the telecommunications carrier or its agent a valid photo ID matching the customer's account information.
(e) Establishment of a Password and Back-up Authentication Methods for Lost or Forgotten Passwords. To establish a password, a telecommunications carrier must authenticate the customer without the use of readily available biographical information, or account information. Telecommunications carriers may create a back-up customer authentication method in the event of a lost or forgotten password, but such back-up customer authentication method may not prompt the customer for readily available biographical information, or account information. If a customer cannot provide the correct password or the correct response for the back-up customer authentication method, the customer must establish a new password as described in this paragraph.

(f) Notification of account changes. Telecommunications carriers must notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed. This notification is not required when the customer initiates service, including the selection of a password at service initiation. This notification may be through a carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record, and must not reveal the changed information or be sent to the new account information.

(g) Business customer exemption. Telecommunications carriers may bind themselves contractually to authentication regimes other than those described in this section for services they provide to their business customers that have both a dedicated account representative and a contract that specifically addresses the carriers' protection of CPNI.

Sec. 64.2011 Notification of customer proprietary network information security breaches.
(a) A telecommunications carrier shall notify law enforcement of a breach of its customers' CPNI as provided in this section. The carrier shall not notify its customers or disclose the breach publicly, whether voluntarily or under state or local law or these rules, until it has completed the process of notifying law enforcement pursuant to paragraph (b) of this section.

(b) As soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach, the telecommunications carrier shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through a central reporting facility. The Commission will maintain a link to the reporting facility at http://www.fcc.gov/eb/cpni.

(1) Notwithstanding any state law to the contrary, the carrier shall not notify customers or disclose the breach to the public until 7 full business days have passed after notification to the USSS and the FBI except as provided in paragraphs (b)(2) and (b)(3) of this section.

(2) If the carrier believes that there is an extraordinarily urgent need to notify any class of affected customers sooner than otherwise allowed under paragraph (b)(1) of this section, in order to avoid immediate and irreparable harm, it shall so indicate in its notification and may proceed to immediately notify its affected customers only after consultation with the relevant investigating agency. The carrier shall cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification. (3) If the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct the carrier not to so disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify the carrier when it appears that public disclosure or notice to affected customers will no longer impede or compromise a criminal investigation or national security. The agency shall provide in writing its initial direction to the carrier, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security and such writings shall be contemporaneously logged on the same reporting facility that contains records of notifications filed by carriers.

(c) customer notification. After a telecommunications carrier has completed the process of notifying law enforcement pursuant to paragraph (b) of this section, it shall notify its customers of a breach of those customers' CPNI.

(d) Recordkeeping. All carriers shall maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to paragraph (b) of this section, and notifications made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach the Company shall retain the record for a minimum of 2 years.

(e) Definitions. As used in this section, a˙breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.

(f) This section does not supersede any statute, regulation, order, or interpretation in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this section, and then only to the extent of the inconsistency.